

## UNITED STATES DISTRICT COURT

for the

Southern District of Texas

APR - 4 2016

David J. Bradley, Clerk of Court

United States of America )

v. )

Robert Romeo Cristea )

Case No.

H16-487 M

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of N/A in the county of Harris in the  
Southern District of Texas, the defendant(s) violated:

Code Section

Offense Description

In or about February 2016, within the Southern District of Texas, defendant, Robert Romeo Cristea, and others known and unknown, did knowingly and willfully combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit: to commit violations of 18 U.S.C. § 1029(a)(2), (b)(2) & (c)(1)(A)(i) (knowingly and with intent to defraud, trafficked in and used one or more unauthorized access devices during any one-year period, and by such conduct obtained anything of value aggregating \$1,000 or more during that period where such offense affected interstate and foreign commerce), all in violation of 18 U.S.C. § 371. ☒

This criminal complaint is based on these facts:

Please see the attached affidavit.

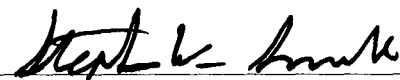
☒ Continued on the attached sheet.


Complainant's signature

FBI Special Agent David Ko

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/04/2016


Judge's signature

City and state: Houston, Texas

Magistrate Judge Stephen W. Smith

Printed name and title

United States Courts  
Southern District of Texas  
FILED

APR -4 2016

David J. Bradley, Clerk of Court

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF TEXAS  
HOUSTON DIVISION

United States of America,  
Plaintiff,

v.

Robert Romeo Cristea,  
Defendant.

Case No. \_\_\_\_\_

H16-487 M

USAO No. 2016R5498

**COMPLAINT**

I, David James Ko, being first duly sworn, hereby depose and state as follows:

**COUNT ONE**  
**Conspiracy to Commit Access Device Fraud**

In or around February 2016, in the Southern District of Texas and elsewhere, defendant

**ROBERT ROMEO CRISTEA**

and others known and unknown, did knowingly and willfully combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit: to commit violations of 18 U.S.C. § 1029(a)(2), (b)(2) & (c)(1)(A)(i) (knowingly and with intent to defraud, trafficked in and used one or more unauthorized access devices during any one-year period, and by such conduct obtained anything of value aggregating \$1,000 or more during that period where such offense affected interstate and foreign commerce), all in violation of 18 U.S.C. § 371.

**THE OBJECTIVE OF THE CONSPIRACY**

The objective of the conspiracy was to steal money from victims' bank accounts by first stealing the victims' ATM card information and PINs.

## **OVERT ACTS**

To further this conspiracy and to effect its illegal objectives, defendant committed the following overt acts in the Southern District of Texas, and elsewhere:

- a. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #1.
- b. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #2.
- c. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #3.
- d. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #4.
- e. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #5.
- f. On or about February 21, 2016, Cristea knowingly used an unauthorized access device to illicitly access the bank account of Victim #6.

## **Summary**

Romeo Cristea, along with several co-conspirators, were observed illicitly withdrawing cash from the accounts of bank customers without their authorization. He was also found possessing card skimming devices which were likely installed on ATMs, allowing he and his conspirators to steal ATM card numbers and PINs. As such, the FBI now seeks an arrest warrant.

## **Introduction and Agent Background**

1. Your Affiant, David Ko, is employed as a Special Agent of the Federal Bureau of Investigation (FBI), and assigned to the Cyber squad in the Houston, Texas division. Affiant has been employed by the FBI since July 2010. As a Special Agent of the FBI, Affiant is charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. More specifically, Affiant investigates cybercrimes involving the unauthorized intrusion into a computer or network and certain technology-related frauds. As part of Affiant's responsibilities as an FBI Agent, Affiant has attended various classes and training. For example, in addition to 20 weeks at the FBI Academy as a Special Agent, I have taken courses in Cyber Investigative Techniques and Resources.

2. The facts set forth in this affidavit are based upon Affiant's own personal observations, training and experience, as well as information obtained during this investigation from other sources, including: (a) other agents from the FBI, and other law enforcement personnel involved in this investigation, (b) statements made or reported by various witnesses with personal knowledge of relevant facts; and (c) my review of records obtained during the course of this investigation, as well as summaries and analyses of such documents and records that have been prepared by others.
3. I make this affidavit in support of an application for a warrant to arrest the defendant for violating 18 U.S.C. § 371 (conspiracy to commit access device fraud) (the Subject Offense). Because this affidavit is submitted for the limited purpose of obtaining this arrest warrant, I have not set forth each and every fact I have learned in connection with this investigation. Where conversations and events are referred to herein, they are related in substance and in part, and where figures and calculations are set forth herein, they are approximate.

#### **ATM Skimming Devices and PIN-Capturing Devices**

4. Based on my training, my experience and information obtained through this investigation, Affiant is aware that ATM skimming "jobs" at a particular bank are typically conducted by groups of two or more individuals. A larger ATM conspiracy may involve several groups of individuals operating at different banks in different geographic areas.
5. Two devices are generally required: (a) a skimming device and (b) a Personal Identification Number ("PIN")-capturing device.
  - (a) A skimming device is an electronic device that can read magnetic strips on the backs of bank cards. A member of the conspiracy typically places the skimming device over the card insertion slot of the ATM or at the ATM lobby doors that control access to the bank lobby with a customer swipe card. While the skimming device is in place, it captures the magnetic strip information of any card that is swiped through the machine. The skimming device will remain on the machine for a period of time until the participants in the skimming scheme remove it.
  - (b) ATM skimmers also typically use PIN-capturing devices in order to steal bank customers' PIN access codes. The PIN-capturing device is installed on or near the ATM and in close proximity to the legitimate, factory-installed PIN pad of the ATM. ATM skimmers typically secure the PIN-capturing device to the machine by using double sided tape and/or superglue. Many PIN-capturing devices, as in this case, use pinhole cameras – tiny easily concealable cameras to capture a customer's PIN number as the customer punches the numbers into the factory-installed PIN pad of the ATM. The device will remain on or near the machine for a period of time until the participants in the scheme remove it.
6. ATM skimmers also typically use computers to download both the video files that captured customers entering account PIN numbers and the bank account information

from the skimming device, and also use a re-encoding device to re-encode that bank account information onto other cards with magnetic strips. The newly encoded card will act as a "clone" of the customer's authentic card. ATM skimmers are also increasingly using Bluetooth technology in ATM skimming devices. This technology allows conspirators to evade detection by remotely transferring the captured data to other electronic devices so that it can later be encoded onto counterfeit "clone" cards.

7. ATM skimmers then steal bank customers' money by using the "clone" cards and stolen PINs to make unauthorized withdrawals from customers' bank accounts.
8. ATM skimming participants, when stopped by law enforcement, often possess large amounts of cash representing the proceeds of their illegal activity. Because those proceeds are derived largely by withdrawing money from ATMs, much of the cash proceeds are in \$20 denominations. In addition, ATM skimmers may possess or have in their vehicles certain tools used to conduct the skimming activity including, for example, double-sided tape, screwdrivers, superglue, and x-acto style knives that allow them to unobtrusively attach skimming devices and PIN-capturing devices.
9. As described above, ATM skimmers use computers to download bank account information from the skimming devices and download video files from video capturing devices. ATM skimmers also use laptop computers and re-encoding devices to transfer the stolen information to "clone" cards. Likewise, stolen information can be stored on smart phones (particularly, if the conspirators use a Bluetooth-enabled PIN-capturing device).

#### **Facts Supporting Probable Cause**

10. Cristea was arrested on Friday, Feb. 26, 2016 based on a state arrest warrant. Cristea has over stayed his visa, and thus is illegally present in the United States.
11. In the days leading up to his arrest, FBI surveillance (and myself) observed Cristea driving a red Toyota RAV4 bearing Texas License Plate DW2141 that, according to an Avis employee, was rented to Romeo Cristea since around February 15, 2016. (For brevity, I may refer to this as Cristea's RAV4.)
12. Affiant, along with the members of an FBI Surveillance Unit, have observed him drive this vehicle and park it at 10615 Meadowglen Lane, Houston, Harris County, Texas where he apparently has been staying overnight in Apt. 310.

**On February 21, 2016, FBI surveillance observes Cristea and Co-conspirator #1 illicitly withdrawing cash at numerous ATMS; these withdrawals were later confirmed to be without authorization**

13. On the morning of February 21, 2016, FBI surveillance observed Romeo Cristea and Co-conspirator #1 drive away from the Meadowglen residence in Cristea's RAV4. Cristea and Co-conspirator #1 went directly to an ATM at a Valero gas station at 1816 Shepherd Drive, Houston, Texas 77007. At approximately 7:36 am (time according to surveillance), Cristea was observed withdrawing cash from that ATM. After Cristea

returned to the RAV4, Co-conspirator #1 proceeded to the ATM and withdrew cash. Between 7:31 am and 7:45 am (time according to records provided by CardTronic, the ATM provider), seven First National Bank accounts were accessed and a total of \$3,109.50 was taken. The FBI talked with First National Bank which confirmed that they had talked with the account holders and confirmed these withdrawals occurred without the owners' consent.

14. Cristea and Co-conspirator #1 continued to steal money that day. At approximately 7:50 am, Cristea and Co-conspirator #1 arrived at a Walmart located at 111 Yale Street, Houston, Texas 77007. An FBI employee observed Cristea walking to the ATM where he used several cards to withdraw cash. Co-conspirator #1 was also later observed using the same ATM to withdraw cash. This ATM was operated by Woodforest National Bank. The suspects then drove away in Cristea's RAV4.
15. Sgt. Gorski contacted Woodforest National Bank Fraud Investigator Bobby Persky who reviewed surveillance video from the ATM transactions that occurred on February 21, 2016, at the aforementioned Woodforest National Bank ATM. According to Investigator Persky, the suspect identified as Cristea conducted seven (7) ATM transactions with debit cards and withdrew cash, and that the suspect identified as Co-conspirator #1 also used multiple debit cards to withdraw cash. However, Investigator Persky stated that none of the account numbers were issued by Woodforest National Bank.
16. Sgt. Gorski is a task force officer with the U.S. Secret Service Electronic Crimes Task Force who helped verify that the accounts accessed by Cristea were issued by First National Bank of Texas. Sgt. Gorski contacted First National Bank of Texas Fraud Investigator Elmo Cepeda who confirmed that these account numbers were issued by First National Bank of Texas and provided the account holders' personal information so the FBI could follow up.
17. Sgt. Gorski contacted six of the account holders who all advised that they still had possession of their First National Bank of Texas debit cards and did not give anyone authorization to use or possess their identifying information.
18. At around 11:09 am that same day, the FBI observed Cristea and Co-conspirator #1 return to the Meadowglen apartment.
19. Cristea's ties to Co-conspirator #1 and #2 are verified by, among other things, the fact that they freely drove Cristea's RAV4 and stayed in the same apartment. For example, at 12:23 pm, the FBI then observed Co-conspirator #1 and Co-conspirator #2 leave the Meadowglen apartment, get into Cristea's RAV4, and drive to a Bank of America located at 11288 Westheimer. Co-conspirator #2 conducted a walk-up ATM transaction and returned to the vehicle. He then moved from the front passenger seat to the driver's side backseat. The FBI then observed their RAV4 drive through the Bank of America drive-thru ATM where defendant Co-conspirator #2 conducted one transaction which the FBI later verified with the bank as a cash deposit that Co-conspirator #2 made into his bank account.



20. Altogether, on February 21, 2016, FBI surveillance observed Cristea, Co-conspirator #1, and Co-conspirator #2 go to approximately 12 different locations, where, according to CardTronic's records, they withdrew at least \$7,000 from at least 18 First National Bank accounts.

**On February 23, 2016, Cristea was observed opening a package which contained white plastic cards**

21. On February 23, 2016 around 12:42 pm, the FBI observed Cristea at a UPS store that he had previously visited several times. Cristea pulled two white envelopes from box 238 and collected approximately 6 boxes from the customer service desk. While at the desk, he opened one of the boxes which contained white plastic cards.
22. These cards are consistent with the fact that once people who engage in the Subject Offenses have stolen victims' ATM card information, they often need blank cards on which to encode this information. In fact, FBI surveillance has reported that they had seen the conspirators use similar white plastic cards during numerous ATM cashouts.

**On February 25, 2016, Cristea dropped off bags at his storage unit**

23. According to records from BullsEye Storage at 1715 Airline Drive, Cristea has been renting unit S0130 since November 2015.
24. On February 25, 2016, FBI surveillance units followed Cristea as he drove his RAV4 from his Meadowglen apartment to BullsEye Storage located at 1715 Airline Boulevard. As FBI surveillance watched, Cristea exited his vehicle with one medium sized black bag with red piping, one gray toolbox, and one white plastic grocery bag. Cristea carried all three items into the storage facility. After several minutes, Cristea was observed leaving the facility without any of the previously mentioned items.
25. Later, the FBI obtained a warrant to search this storage unit and recovered, among other things: four credit card skimmers, hundreds of magnetic stripe gift cards, computers, cell phones, and cash.

**On Friday, February 26, 2016, the FBI arrested Cristea and executed a search warrant on his Meadowglen apartment**

26. On Friday, February 26, 2016, the FBI arrested Cristea. Notably, when arrested, Cristea mentioned that he was on his way to Atlanta.
27. In Cristea's RAV4, the following items, among others, were recovered:
- 2 ATM Skimmers, black outer coating false card inserts (plastic bag / large luggage)
  - Black & Red Wires, Red Connector, cut USB Charger Sable Cord, 2 finger nail clippers used to cut wire, tweezers & blue L shaped metal tool w/sharp edge w/ black electrical tape (small luggage)
  - Lenovo Edge 15 Laptop, Model 80H1, Serial #R907CKZJ, (small luggage)

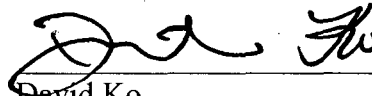
- Sandisk Adapter (black) and SanDisk 8 GB, Micro SD (small luggage)

28. The FBI also executed a search warrant at Cristea's Meadowglen apartment. There, they found items consistent with an ATM skimming scheme such as:

- Lenovo laptop Model 100S, with power-cord, s/n YD008KKW;
- Misc. ATM and Moneygram receipts,
- Gift cards and ATM receipts;
- Exacto knife set, volt-meter, SIM card packages found on kitchen table;
- Garmin GPS Model NUVI 2797LM with charger and stand, s/n 2UE049386;
- Two reloadable cash cards;
- Hitec multi-charger box, screwdriver set; box with batteries;
- Miscellaneous paperwork with IDs and passwords, two Walmart gift cards

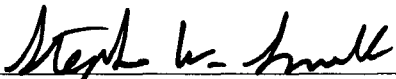
### Conclusion

29. I respectfully submit there is probable cause to believe that Cristea has committed the Subject Offenses. Thus, I request that the Court issue the arrest warrant.



David Ko  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me  
on this 4<sup>th</sup> day of ~~March~~  
April 2016.



U.S. Magistrate Judge Stephen William Smith